The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa

Lukman Adebisi Abdulrauf

Centre for human rights, University of Pretoria, South Africa

&

Charles Manga Fombad

Professor of Law, Institute for International & Comparative Law in Africa, University of Pretoria, South Africa

1. Introduction

- The unregulated processing of individuals' personal information has profound effects on key human rights especially privacy.
- This is so esp. because of Africa's growing ICT sector and its strong desire to build the information society so as to key into globalization process.
- Some regions and international institution have taken action (**with DP instruments**) but Africa has lagged behind until recently with a number of sub regional instruments and more recently, regional instrument
- Data protection is a subject that requires a great deal of harmonization for effectiveness- because of TBDF.
  - Its human rights affiliations is also no longer in doubt
- Thus, the AU Convention on Cybersecurity and Personal Data Protection 2014, deserves further comments especially its data protection provisions – so as to determine if it is indeed a possible cause for celebration of human rights in Africa. In determining, consider:
  - Are its provisions in tandem with international prescripts on dp
  - What are the possible obstacles it may face in realizing dp on the continent

1. Introduction (Cont'd)

- The presentation is organized in 5 parts, *viz*
  - 1 Introduction
  - 2 Why regional data protection instrument is necessary: The information society in Africa and human rights challenges
  - 3 Analysing the substantive aspects of the AU Convention: Comparing with "long standing" & "influential" instruments esp the CoE Convention (& Sometimes, the EU Directive)
  - 4 (Possible) challenges of the Convention in realization of the right to data protection
  - 5 Conclusion

2. Building Africa's information society and challenge of human rights protection

- Africa is making strenuous efforts at various levels to build the **information society** (IS). See eg initiatives like AISI & ARAPKE
  - Realization of the immense value of information – "information is a crucial economic and social resources'
  - Benefits of the IS: globalization, economic & social development
- Two major features of an information society are: proliferation of ICTs & increase in demand for PI by various entities
- Challenges of IS: both feature put together could lead to loss of control over PI by individuals thus, human rights violation esp in
  - 1. Proliferation on internet & online services
    - With an estimated population of over 1billion, Africa has more that 300million internet users thus, more than 30% internet penetration

2. Building Africa's information society and challenge of human rights protection

- 2. National ID card schemes: according to Banisar, 'The most common ICT privacy issue currently facing African nations is the development of new citizen identification systems, including identity cards and passports'. Nowadays, proliferation of e-ID cards
- 3. SIM card registration exercise: …without an enabling legal framework for the protection of PI
- 4. Surveillance technologies

3. Group initiatives on dp prior to the AU Convention

- A number of countries with dp legislation (15, by 2016) however, this cannot solve dp issues resulting from TBDF thus, subregional initiatives
- REC's championed subregional initiatives: thus, 4 RECs have made effort on dp
  - 1. ECOWAS, with ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS (2010). "Leading initiative on dp in Africa". The Act is legally binding on member states as it is annexed to and forms part of the ECOWAS Treaty. (Art 48). Applies directly in *monist* states
  - 2. EAC, with the EAC Legal Framework for Cyber Laws (Phase 1 & 2) 2008/2011. however, the Legal Framework is not legally binding unlike ECOWAS. It merely contains a series of recommendations. Para 2.5 contains recommendations on 'data protection and privacy' but no content principles or minimum standard.
  - SADC, with SADC Model Law, 2012. Gave prescriptive guidance to member states in enacting dp law however, not binding.

3. Group initiatives on dp prior to the AU Convention

- ECCAS/CEMAC, with a model law containing 3 texts on electronic transactions, dp and cybercrime. Also, non-binding.

- The above initiatives have, according to scholars, indicated that Africa is now leading the global expansion of dp law.
- However, these initiative may not be a credible alternative for a *unified* regional framework on dp. Hence, the AU DP Convention

4. The AU Data Protection Convention

- AU is properly suited because it is Africa's regional system for promotion and protection of human rights
- **Background to the Convention**
  - before the Convention, there were a number of drafts in 2011 &2013. the Draft AU Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa. Another draft was the AU Convention on the Confidence and Security in Cyberspace. These drafts were heavily criticized by advocacy groups
  - In May 2014, these drafts were reviewed in a meeting of experts from the AU member states' ministry of justice.
  - On 27 June 2014, the AU Convention was adopted at the 23rd Ordinary session of the AU Submit in Malabo.
  - The Convention has a broad scope to cover 3 important IT subjects : electronic transactions, dp & cybercrime.

4. The AU Data Protection Convention

- **Objective and purpose of the Convention**
- 2 broad objectives: (arts 8(1) & (2)) Commits state parties to 1) establish a legal framework for strengthening fundamental, particularly the physical data and punish privacy violation without prejudice to the principle of free flow of data. 2) such a framework shall ensure respect for fundamental rights while recognizing other interests in PI such as the interest of state, local communities and businesses
  - **Discussion**
  - Objective, like the CoE Convention, shows a clear human rights agenda as human rights protection comes out more strongly
  - Explicitly recognizes other interest in PI
  - Issues: obscure terms like physical data, local communities
  - Unlike the CoE Convention in art 1, AU Convention is not explicit on whether the legal framework so established by states should be applicable only citizens of member states.

    Issues with privacy as a core objective of the AU Convention.

4. The AU Data Protection Convention

- **Scope and application**
  - art 9(c) applicable to any *processing* carried out in the territory of a state party. Ie all the 54 African countries with the exception of Morocco
  - Processing according to art 1 is any operation performed on personal data whether or not by automatic means. Unlike the CoE Convention, AU applies to both automated and manual processing
  - PI is also important to determine scope. "jurisdictional trigger". PI is defined in art 1 as 'information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly…' substantial replication of the EU Directive.
  - Unlike other data protection instruments, the AU Convention, in art 9(d), places 'any processing of data relating to public security, defence, research, criminal prosecution or state security' within its scope. However, subject to 'exceptions defined by specific provisions of other extant laws'. Compare with art 3(2) EU Directive…outright exclusion. CoE also has a similar provision like the AU Convention,

4. The AU Data Protection Convention

- The AU Convention is not applicable to processing for personal or household activates. Also, the Convention does not apply to 'temporary copies produced within the context of technical activities for transmission and access to a digital network with a view to automatic, intermediate and temporary storage.' art 9(2). Unclear exception however, arguably based on *de minimis*
- The AU Convention contains little exemptions unlike many data protection instruments.

- **Fair information Practices/Principles**
- See sec III titled 'obligations relating to conditions governing data processing'
- Principles, unlike other instruments, are set out in a specific fashion
- 6 principles influenced by a combination of the OECD Guidelines & EU Directive
  - 1 principle of consent and legitimacy of personal data processing: *opt in* consent

4. The AU Data Protection Convention

- 2 Principle of lawfulness and fairness of personal data processing. Also in the CoE Conv
- 3 principle of purpose, relevance and storage of processed personal data. Also in the CoE Conv
- 4 Principles of accuracy of personal data also in the CoE Convention
- 5. principle of transparency of personal data processing not in either CoE Convention or EU Directive. Contained in both reform documents (art 7bis of CoE proposal & arts 5(a) & 11 of draft EU Regulation
- 6. principle of confidentiality and security of personal data processing. Not as explicit as the CoE Convention in that data controllers must put in place appropriate security measures. Also, like the CoE Convention, no obligation for data breach notification. (see art 7(b) Proposal & 31 draft EU Regulation
- There is no accountability principle.
- **Sensitivity**, art 14 AU Convention: listed category appears to b closed. In any case, the relevance of specific provisions on sensitivity have been question. "risk not on the content of data but on the context used"

4. The AU Data Protection Convention

- **Specific rights of data subjects and duties of data controllers**
- AU Convention contains rights to information, access, object & rectification or erasure in arts 16-19 respectively. Superfluous? 'a right and duty are correlative and inseparable' ?Eg right to information in art 16 has the same effect as the principle of transparency (principle 5)
- No specific provision for rights in the CoE Convention, however, it is contained in the proposal for modernization. So also the EU Directive & draft EU Regulation
- The AU Convention still outlines some obligations of data controller (sec V) eg confidentiality, security, storage and substantial obligations. This is clearly superfluous as sect III contains obligations. No similar provision in either the CoE Convention or EU Directive
- Obligation in art 23 of AU Convention , 'sustainability obligations' is strange. Data controller should take all appropriate measures to ensure that processed personal data can be utilized'

4. The AU Data Protection Convention

- **Regime of TBDF**
- Art 14(6) of the AU Convention. A data controller is prohibited from transferring personal data to a non-member state of the AU without an 'adequate level of protection of privacy, freedoms and fundamental rights'
- Issues: positioning of the provision- under sensitive data; scanty provision- what is adequate? How should it be determined?; no exceptions where data can be transferred to a country without an 'adequate' regime. See CoE Convention, art 2(2) of the additional protocol to the Convention)

- **Oversight & enforcement**
- art 11 (1), AU requires that member states must establish independent institutional frameworks to protect PI - NPAs.

  The Convention contains very robust provisions on their duties and powers

4. The AU Data Protection Convention

- The Convention also require that NPA's must establish mechanisms for cooperation with DPAs in third countries. However, no specific provision for NPAs to cooperate among themselves unlike the CoE Convention in art 1(5) of the Additional Protocol (see also art 28(6) EU Directive)

5. Some reflections on possible challenges of the AU Convention

- 2 major categories of problems: Problems with the Convention itself & other general problems
- **Inherent problems of the Convention**
  - 1. Broad scope: 3 different chapters - electronic transactions, dp and cybersecurity. Hence scattered provisions eg direct marketing
  - Confusion that may arise when a state party is only interested in one of the subject matters: ie Can a state party ratify only the dp aspect and leave out the rest.
  - So much attention on other aspects at the expense of human rights: eg cybersecurity
  - 2. ambiguous & confusing provisions: "local communities". Art 10 "preliminary formalities"? declaration, authorization
  - Inconsistent provisions: personal data, electronic data, physical data, computerized data
  - Omissions: Data breach notifications, PIA

5. Some reflections on possible challenges of the AU Convention

- 3. No provision establishing supervisory authority at the regional level. Art 32 merely provides that AU Commission Chairperson is responsible for implementation. CoE 'Consultative Committee', EU Directive Art 29 WP
- 4. 'broad fashion' style adopted for member states to domesticate or incorporate however, effects on harmonization, also no requirement that Conventions provision is minimum.

- **Other problems**
  - 1 African problem towards international (human rights) treaties.
    - Ratification issues – no state party is yet to ratify & 15 African Countries is needed to come into force
    - Ratification without implementation: complicated by dualist structure existing in most member states
    - Compliance: Viljoen 'the greatest challenge [in Africa] is to bring about compliance with treaty provisions by governments officials and nationals alike'

5. Some reflections on possible challenges of the AU Convention

- 2 General African attitude towards privacy: privacy is a western idea of individualism. Africans suffer from "privacy myopia". Bakinbinga. This idea has been criticized severely.
- 3. competition with other dp regimes: esp EU Directive. Also RECs. Thus AU Convention must harmonize regional initiatives.

6. Conclusion

- 2016 is a very significant year for human rights in Africa: 35th anniversary of adoption of ACHPR, 30th anniversary of entering into force of the Charter,10th anniversary of the operationization of the African court.
- The international community will therefore pose some critical questions regarding the state of human rights on the continent. An important question is how human rights have fared in the face of relative advances in technology. Privacy and dp will definitely be the focus.
- The Convention is indeed a laudable initiative of the AU esp in the human rights perspective. Regarding if it calls for celebration of human rights must be determined on two levels
  - Firstly, is it in accordance with international dp laws – By and large, it is. On this level therefore, the convention is an important addition to the jurisprudence of human rights

6. Conclusion

- Secondly, and most importantly, is implementation and compliance. Here lies the problem
- **Recommendations:** Value change on data protection and privacy in Africa, responsibility of African leaders,

THANK YOU FOR YOUR ATTENTION